CYBERVIEW SECURITY OVERVIEW:

Red River's Secure-ED K12 Solution Set

Red River

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. **THINK RED.**

Protecting Our Schools

Over the past 3 years there has been a dramatic increase in K-12 cybersecurity incidents and all indications show no signs of these breaches slowing down. Each attack runs the risk of exposing students' personal information or confidential administrative data, both which can have far-reaching consequences. It is therefore imperative that school systems adequately protect their data, have the capability to notify leadership when a breach has occurred and relate that breach to the severity of the incident.

More than two-thirds of school districts' educational technology leaders say data privacy and security are more important than ever, according to a recent national survey by the Consortium for School Networking. Key areas of concern are driven by ransomware and phishing attacks that have cost districts hundreds of thousands of dollars. These attacks also divert time and money away from programs designed to comply with state and federal data privacy laws requiring protection of student records, further exposing districts to risk.

To keep pace with the evolving threat landscape, K-12 districts must continuously progress in the highest areas of risk requiring the most critical of cybersecurity protection. New approaches in security assessments, concerns over security and privacy, and reimagining how districts provide security policy, security technology and monitoring services are among factors that will drive K-12 cyber security programs over the coming year.

Texas SB 820, Setting the Standard

The most common form of K-12 cyberattacks are data breaches. Due to the prevalence of these attacks and the sensitivity of the data at risk, it is imperative school districts in Texas meet or exceed compliance with TX SB 820 and implement the robust associated security practices that protect the information of students and the district network infrastructure.

Published 02/19/2020

SB 820 Requirements

1. Designate a security coordinator
2. Adopt a cybersecurity policy
3. Report any breach of student personally identifiable data to TEA

SB 820 Goals & Functionality

1. Implementing an organization-wide cybersecurity policy to provide:
   - Secure district cyberinfrastructure against cyber-attacks, student PII and other related cybersecurity incidents
   - Determine cybersecurity risk and implement mitigation planning
   - Provide resilience against cyberattacks, monitoring of cybernetwork & student PII
2. Policy to provide resilience against cyberattacks, mentoring of cybernetwork & student PII
3. Oversight and processes for reporting and metrics
4. The cybersecurity coordinator is required to:
   - Report any breach of the district's information systems to the agency.
   - Provide notice to a parent or guardian of a breach that involves a student's PII.

What does this mean for school districts?

TX SB 820 means that school districts are now responsible for handling their own cybersecurity measures, including the identification and reporting of breaches.

While the terms of what this new law entails and what specific components the law will require are still being refined. However, based on our industry experience and understanding of cybersecurity in Texas, requirements will likely include:

- **Creation:** School district security policies will likely align with existing Texas cybersecurity framework solution sets.
- **Testing:** The school district cybersecurity policy implementation will likely be required by this law.
- **Demonstration of effectiveness:** It is important to not only meet the policy to ensure compliance, but to also consider the actual effectiveness of the cybersecurity framework program. These security measures should be practical and effective.

Red River Secure-ED Solution Set

Red River has proven experience in the university and education system with the creation and implementation of extensive security policies and control programs, including:

- Cybersecurity and compliance frameworks (NIST, HIPAA, PCI, FERPA, CCPA)
- Network, application, information and operational readiness security assessments
- Risk management and remediation programs
- Formal security awareness and the protection of personal privacy as well as critical information assets

In addition to security expertise, Red River knows price to value is critical in the K12 environment. To ensure our nation's school districts are getting the most from their security budget, Red River has created the Secure-ED security solution set. Secure-ED is a combination of no-cost security K12 resources, value-priced services, a suite of best practices to ease implementation and suite of bundled security packages designed to maximize every dollar spent.

Red River's security practice engineers are highly certified and equipped with the expertise and solutions needed to help school districts in Texas establish cybersecurity policies that satisfy the requirements of TX SB 820, while protecting the sensitive data of students, the district cybernetwork, faculty and staff.

Secure-ED is a long-term program that is a combined offering of currently available items, additional components added over 2020 and long-term program items.

The following are core Secure-ED services and solutions offered:

K12 Security Policy Info Pack
- TASB Cyber-info links (free)
- RR Streamlined Policy (CIS 20 / NIST CSF) (free)
- Implementation support

K12 Cyber Risk Management
- SB-820 risk mgt cyber sheet (free)
- K-12 Security Best Practices Guide (free)
- RR advanced risk mgt solutions

Cyber Network Monitoring & Containment
- Security incident reporting workflows (free)
- Student PII breach
- Cyber network events
- 24x7 managed service

Secure-Ed Assessment
- K-12 Cyber network security assessment
- ID critical risks
- Remediation plans
- Security roadmap & budget planning

Incident Response Readiness
- Incident Response on Demand (IROD)
- 3 levels of support options

Security Training & Cyber Support
- Secure admins
- Power users
- Cyber leads
- RR Senior HS Cyber-Aware skills program

In addition to core Secure-ED solution components, Red Rivers has optimized the following services and cyber-specific programs:

K-12 Managed Cybersecurity Programs:

What is it?
Cost effective managed security services specially scoped for K12 & SB 820 compliance support.

Program Overview

Cyber Essentials:
- 24x7 Cyber network monitoring & response service
- RR SB 820 Cyber tool kit
- Red River Level 1 Incident Response program

Defensive Pro:
- 24x7 Extended Cyber Network Monitoring & Response Service
- Email security monitoring + Critical end point security monitoring
- Red River Level 2 Incident Response Program

Cyber Elite:
- 24x7 Every Segment Cyber Network Monitoring & Response Service
- Advanced Email security protection & monitoring + Extended end point security monitoring & containment
- Red River Level 3 Incident Response Program

Secure-ED: Posture Assessment Review:

What is it?

- Baseline how secure-ready your K-12 District is
- Roadmap of what needs to be done to achieve the desired goals

Why do I want it?

- ID critical risks
- Create a professional starting point to continuously ID & address Cyber security threats

What do we get for the money?

- Cyber security assessment (internal & external) + Initial Student PII & sensitive data exposures
- K-12 monitoring & response capabilities
- K-12 Dark Web Recon
- ID critical security risks & remediation report by priority
- High-level roadmap & budget planning report

K-12 Cyber Protection Bundle

What is it?

- Firewall Upgrade (Next Gen)
- 24x7 DNS Monitoring (Cisco Umbrella / Palo Alto DNS)
- Bundled Installation Services
- **Optional:** RR Managed Security Services, NGFW, DNS, endpoint & access Mgt

Why do I want it?

- Protect sensitive student, admin and critical data against malware, ransomware and other related threats
- App visibility, next-gen IPS, advanced malware protection and URL filtering work together

What do we get for the money?

- Architecture validation of FW & DNS Security service placement
- Red River professional Installation
- Half- day user training on products and best practices
- 6 mo. follow up check point

For more information, please contact your local Red River K-12 solution specialist.

About Red River

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions.

For more information please call 800.769.3060 or visit **redriver.com**

Follow us on Twitter: **@ThinkRed**